

Admin API Documentation

Overview / نظرة عامة

This document describes the admin API endpoints for comprehensive user management in the Magnet project.

للمدير لإدارة شاملة للمستخدمين في مشروع API هذا المستند يصف نقاط نهاية Magnet.

المصادقة والتفويض / Authentication & Authorization

All admin endpoints require:

- **Authentication:** Valid JWT token in `Authorization: Bearer <token>` header
- **Authorization:** User must have `admin` role

جميع نقاط نهاية المدير تتطلب:

- صالح في رأس JWT **المصادقة:** رمز
- **التفويض:** يجب أن يكون للمستخدم دور `admin`

الرابط الأساسي / Base URL

```
/api/admin
```

نقاط نهاية إدارة المستخدمين / User Management Endpoints

1. Create User / إنشاء مستخدم

POST `/api/admin/users`

Creates any type of user (customer, business, magnet_employee, admin).

مدير، إنشاء أي نوع من المستخدمين (عميل، عمل، موظف).

Request Body / جسم الطلب

```
{
  "firstname": "John",
  "lastname": "Doe",
  "email": "john.doe@example.com",
  "phone": "+966501234567",
  "password": "SecurePassword123",
  "role": "business",
```

```

"country": "Saudi Arabia",
"language": "en",
"crNumber": "CR123456",
"vatNumber": "VAT123456",
"companyName": "Example Company",
"companyType": "LLC",
"city": "Riyadh",
"district": "Al Olaya",
"streetName": "King Fahd Road"
}

```

الحقول المطلوبة حسب الدور / Required Fields by Role

الدور / Role	الحقول المطلوبة / Required Fields
customer	firstname, lastname, email, password, country
business	firstname, lastname, email, password, country, crNumber, vatNumber, companyName, companyType, city, district, streetName
magnet_employee	firstname, lastname, email, password, country
admin	firstname, lastname, email, password, country

الاستجابة / Response

```
{
  "status": "success",
  "data": {
    "user": {
      "id": "60f7b3b3b3b3b3b3b3b3b3b3b3",
      "firstname": "John",
      "lastname": "Doe",
      "email": "john.doe@example.com",
      "phone": "+966501234567",
      "role": "business",
      "country": "Saudi Arabia",
      "language": "en",
      "isEmailVerified": true,
      "isPhoneVerified": true,
      "isDisallowed": false,
      "businessInfo": {
        "crNumber": "CR123456",
        "vatNumber": "VAT123456",
        "companyName": "Example Company",
        "companyType": "LLC",
        "city": "Riyadh",
        "district": "Al Olaya",
        "streetName": "King Fahd Road",
        "isApproved": true,
        "approvalStatus": "approved"
      }
    }
  }
}
```

```

    },
    "createdAt": "2024-01-15T10:30:00.000Z",
    "updatedAt": "2024-01-15T10:30:00.000Z"
  }
},
"message": {
  "en": "User created successfully",
  "ar": "تم إنشاء المستخدم بنجاح"
}
}

```

2. Get All Users / الحصول على جميع المستخدمين

GET /api/admin/users

Retrieves all users with pagination, filtering, and search capabilities.

استرجاع جميع المستخدمين مع الترقيم والتصفية وإمكانيات البحث.

معاملات الاستعلام / Query Parameters

Parameter / المعامل	Type / النوع	Description / الوصف
page	number	Page number (default: 1)
limit	number	Items per page (default: 10)
role	string	Filter by role (<code>customer</code> , <code>business</code> , <code>magnet_employee</code> , <code>admin</code>)
status	string	Filter by status (<code>active</code> , <code>disallowed</code>)
search	string	Search in name, email, phone, company name
sortBy	string	Sort field (default: <code>createdAt</code>)
sortOrder	string	Sort order (<code>asc</code> , <code>desc</code>)

مثال على الطلب / Example Request

```
GET /api/admin/users?
page=1&limit=10&role=business&status=active&search=company&sortBy=createdAt&sortOrder=desc
```

الاستجابة / Response

```
{
  "status": "success",
  "data": {
    "users": [
      {
        "id": "6f5f3a2e-4a2d-4a2d-8a2d-4a2d4a2d4a2d",
        "name": "John Doe",
        "email": "john.doe@example.com",
        "role": "business",
        "status": "active",
        "createdAt": "2024-01-15T10:30:00.000Z",
        "updatedAt": "2024-01-15T10:30:00.000Z"
      }
    ]
  }
}
```

```
{  
    "id": "60f7b3b3b3b3b3b3b3b3b3b3b3b3b3b3",  
    "firstname": "John",  
    "lastname": "Doe",  
    "email": "john.doe@example.com",  
    "phone": "+966501234567",  
    "role": "business",  
    "country": "Saudi Arabia",  
    "language": "en",  
    "isEmailVerified": true,  
    "isPhoneVerified": true,  
    "isDisallowed": false,  
    "businessInfo": {  
        "companyName": "Example Company",  
        "approvalStatus": "approved"  
    },  
    "createdAt": "2024-01-15T10:30:00.000Z"  
}  
]  
},  
"pagination": {  
    "currentPage": 1,  
    "totalPages": 5,  
    "totalItems": 50,  
    "itemsPerPage": 10  
}  
}
```

3. Get User Statistics / الحصول على إحصائيات المستخدمين

GET /api/admin/users/stats

Retrieves comprehensive user statistics.

استرجاع إحصائيات شاملة للمستخدمين.

Response / الاستجابة

```
{  
    "status": "success",  
    "data": {  
        "stats": {  
            "total": 150,  
            "byRole": {  
                "customers": 80,  
                "businesses": 45,  
                "employees": 15,  
                "admins": 10  
            },  
            "byStatus": {  
                "active": 140,  
                "inactive": 10  
            }  
        }  
    }  
}
```

```
        "active": 140,
        "disallowed": 10
    },
    "businessApproval": {
        "pending": 5,
        "approved": 35,
        "rejected": 5
    }
}
}
```

الحصول على مستخدم بالمعرف / Get User by ID

GET /api/admin/users/:id

Retrieves a specific user by their ID.

استرجاع مستخدم محدد بواسطة المعرف.

الاستجابة / Response

```
{
    "status": "success",
    "data": {
        "user": {
            "id": "60f7b3b3b3b3b3b3b3b3b3b3b3b3b3b3",
            "firstname": "John",
            "lastname": "Doe",
            "email": "john.doe@example.com",
            "phone": "+966501234567",
            "role": "business",
            "country": "Saudi Arabia",
            "language": "en",
            "isEmailVerified": true,
            "isPhoneVerified": true,
            "isDisallowed": false,
            "businessInfo": {
                "crNumber": "CR123456",
                "vatNumber": "VAT123456",
                "companyName": "Example Company",
                "companyType": "LLC",
                "city": "Riyadh",
                "district": "Al Olaya",
                "streetName": "King Fahd Road",
                "isApproved": true,
                "approvalStatus": "approved"
            },
            "createdAt": "2024-01-15T10:30:00.000Z",
            "updatedAt": "2024-01-15T10:30:00.000Z"
        }
    }
}
```

```
    }
}
}
```

5. Update User / تحديث مستخدم

PUT /api/admin/users/:id

Updates a user's information.

تحديث معلومات المستخدم

Request Body / جسم الطلب

```
{
  "firstname": "John Updated",
  "lastname": "Doe Updated",
  "email": "john.updated@example.com",
  "phone": "+966501234568",
  "password": "NewSecurePassword123",
  "role": "business",
  "country": "Saudi Arabia",
  "language": "ar",
  "isEmailVerified": true,
  "isPhoneVerified": true,
  "isDisallowed": false,
  "crNumber": "CR123456",
  "vatNumber": "VAT123456",
  "companyName": "Updated Company",
  "companyType": "LLC",
  "businessCity": "Jeddah",
  "businessDistrict": "Al Hamra",
  "businessStreetName": "King Abdulaziz Road"
}
```

Response / الاستجابة

```
{
  "status": "success",
  "data": {
    "user": {
      "id": "60f7b3b3b3b3b3b3b3b3b3b3b3b3",
      "firstname": "John Updated",
      "lastname": "Doe Updated",
      "email": "john.updated@example.com",
      "phone": "+966501234568",
      "role": "business",
      "country": "Saudi Arabia",
    }
  }
}
```

```

    "language": "ar",
    "isEmailVerified": true,
    "isPhoneVerified": true,
    "isDisallowed": false,
    "businessInfo": {
        "crNumber": "CR123456",
        "vatNumber": "VAT123456",
        "companyName": "Updated Company",
        "companyType": "LLC",
        "city": "Jeddah",
        "district": "Al Hamra",
        "streetName": "King Abdulaziz Road",
        "isApproved": true,
        "approvalStatus": "approved"
    },
    "createdAt": "2024-01-15T10:30:00.000Z",
    "updatedAt": "2024-01-15T11:30:00.000Z"
},
{
    "message": {
        "en": "User updated successfully",
        "ar": "تم تحرير المستخدم بنجاح"
    }
}

```

6. Delete User / حذف مستخدم

DELETE /api/admin/users/:id

Deletes a user permanently.

حذف المستخدم نهائياً.

Response / الاستجابة

```
{
    "status": "success",
    "message": {
        "en": "User deleted successfully",
        "ar": "تم حذف المستخدم بنجاح"
    }
}
```

7. Disallow User / منع مستخدم

PUT /api/admin/users/:id/disallow

Disallows a user from logging in or performing actions.

منع المستخدم من تسجيل الدخول أو تنفيذ الإجراءات.

Request Body / جسم الطلب

```
{
  "reason": "Violation of terms of service"
}
```

Response / الاستجابة

```
{
  "status": "success",
  "data": {
    "user": {
      "id": "60f7b3b3b3b3b3b3b3b3b3b3b3b3b3b3",
      "firstname": "John",
      "lastname": "Doe",
      "email": "john.doe@example.com",
      "role": "business",
      "isDisallowed": true,
      "disallowReason": "Violation of terms of service",
      "disallowedBy": "60f7b3b3b3b3b3b3b3b3b3b3b4",
      "disallowedAt": "2024-01-15T12:00:00.000Z",
      "updatedAt": "2024-01-15T12:00:00.000Z"
    }
  },
  "message": {
    "en": "User disallowed successfully",
    "ar": "تم منع المستخدم بنجاح"
  }
}
```

8. Allow User / السماح للمستخدم

PUT /api/admin/users/:id/allow

Allows a previously disallowed user to login and perform actions.

السماح للمستخدم محظوظ سابقاً بتسجيل الدخول وتنفيذ الإجراءات.

Response / الاستجابة

```
{
  "status": "success",
  "data": {
    "user": {
      "id": "60f7b3b3b3b3b3b3b3b3b3b3b3b3b3b3",
      "firstname": "John",
      "lastname": "Doe",
      "email": "john.doe@example.com",
      "role": "business",
      "isDisallowed": false,
      "disallowReason": null,
      "disallowedBy": null,
      "disallowedAt": null,
      "updatedAt": "2024-01-15T12:00:00.000Z"
    }
  }
}
```

```

    "id": "60f7b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3",
    "firstname": "John",
    "lastname": "Doe",
    "email": "john.doe@example.com",
    "role": "business",
    "isDisallowed": false,
    "allowedBy": "60f7b3b3b3b3b3b3b3b3b3b3b3b3b3b4",
    "allowedAt": "2024-01-15T13:00:00.000Z",
    "updatedAt": "2024-01-15T13:00:00.000Z"
  }
},
"message": {
  "en": "User allowed successfully",
  "ar": "تم السماح للمستخدم بنجاح"
}
}

```

استجابات الأخطاء / Error Responses

رموز الأخطاء الشائعة / Common Error Codes

Status Code / رمز الحالة	Description / الوصف
400	Bad Request - Invalid input data
401	Unauthorized - Missing or invalid token
403	Forbidden - Insufficient permissions
404	Not Found - User not found
500	Internal Server Error

مثال على استجابة الخطأ / Example Error Response

```
{
  "status": "error",
  "message": {
    "en": "User not found",
    "ar": "المستخدم غير موجود"
  }
}
```

اعتبارات الأمان / Security Considerations

حماية المدير / Admin Protection

- Admins cannot delete themselves

- Admins cannot disallow themselves
- All admin actions are logged
- Strong password requirements enforced

منع المستخدمين / User Disallowance

- Disallowed users cannot login
- Disallowed business users cannot add products
- Disallowed users cannot perform any actions
- Disallowance reason is tracked

أمثلة الاستخدام / Usage Examples

إنشاء مستخدم عمل / Create a Business User

```
curl -X POST /api/admin/users \
-H "Authorization: Bearer <admin_token>" \
-H "Content-Type: application/json" \
-d '{
  "firstname": "Ahmed",
  "lastname": "Al-Sayed",
  "email": "ahmed@company.com",
  "phone": "+966501234567",
  "password": "SecurePass123",
  "role": "business",
  "country": "Saudi Arabia",
  "crNumber": "CR789012",
  "vatNumber": "VAT789012",
  "companyName": "Al-Sayed Trading Co.",
  "companyType": "LLC",
  "city": "Riyadh",
  "district": "Al Olaya",
  "streetName": "King Fahd Road"
}'
```

الحصول على المستخدمين مع المرشحات / Get Users with Filters

```
curl -X GET "/api/admin/users?
role=business&status=active&search=company&page=1&limit=10" \
-H "Authorization: Bearer <admin_token>"
```

منع مستخدم / Disallow a User

```
curl -X PUT /api/admin/users/60f7b3b3b3b3b3b3b3b3b3b3/disallow \
-H "Authorization: Bearer <admin_token>" \
-H "Content-Type: application/json" \
```

```
-d '{  
    "reason": "Multiple terms of service violations"  
}'
```

Notes / ملاحظات

1. **Business Users:** When creating business users, they are automatically approved
2. **Password Security:** All passwords are hashed using bcrypt
3. **Email Verification:** Admin-created users are automatically email verified
4. **Phone Verification:** Admin-created users with phone numbers are automatically phone verified
5. **Disallowance:** Disallowed users cannot perform any actions in the system
6. **Audit Trail:** All admin actions are tracked with timestamps and admin IDs

مستخدمي الأعمال: عند إنشاء مستخدمي الأعمال، يتم الموافقة عليهم تلقائياً.

أمان كلمة المرور: جميع كلمات المرور مشفرة باستخدام bcrypt.

التحقق من البريد الإلكتروني: المستخدمون المنشأون من قبل المدير يتم التحقق من بريدهم الإلكتروني تلقائياً.

التحقق من الهاتف: المستخدمون المنشأون من قبل المدير مع أرقام الهاتف يتم التتحقق من هواتفهم تلقائياً.

المنع: المستخدمون المحظوظون لا يمكنهم تنفيذ أي إجراءات في النظام.

مسار التدقيق: جميع إجراءات المدير يتم تتبعها مع الطوابع الزمنية ومعرفات المدير.